



STI Wireless Network Policy

Overview

Wireless Network and Internet Access are available throughout buildings on Southeast Technical Institute's (STI) campus. Due to the nature of wireless communication, wireless networking requires cooperation between faculty, staff and students in order to fully maximize the benefits of wireless technology.

The wireless network was designed for educational use on campus. The wireless network is a shared resource and is intended to supplement and enhance the existing wired network, not replace it.

Purpose

The purpose of this policy is to inform the user about the acceptable use of the wireless network at STI. This policy has been put in place to protect the staff, faculty, and students; to prevent inappropriate use of wireless network access that may expose STI to multiple risks including viruses, network attacks, and various administrative and legal issues.

This policy has been created to expand on the STI's Technology Resource Policy and Acceptable Use Policy by including specific information regarding the use of wireless networking and data access on campus.

Scope

This Wireless Usage policy applies to any and all wireless devices and software applications used on campus. It also applies to all staff, faculty, students, and guests at STI. The purpose of this policy is to ensure the security, reliability and utilization of the wireless network.

General Use

It is the intention of STI's IT Department to provide a high level of reliability and privacy when using the wireless network. Wireless Access Points are distributed across STI's campus in order to provide and maintain connectivity with buildings on campus. Wireless Access Points provide a shared bandwidth. As the number of users increase the available bandwidth per user decreases. Please show consideration for other users and refrain from running high bandwidth applications and operations such as downloading large music files and video from the Internet. Network reliability is determined by the level of user traffic and accessibility. In order to provide an acceptable level of reliability, bandwidth will be regulated according to the application.

STI's IT Department cannot guarantee the confidentiality of any information stored on any device belonging to STI's or connected to the STI's Wireless Network.



Access

STI Wireless Network (Secured)

The Southeasttech Wireless Network is STI's secured wireless network. Through this network, all campus resources such as printing and datacluster are available. This network is only accessible to students and employees on STI owned machines. Students who complete a conditional sales agreement and receive a laptop through STI will have access.

In order to access the Southeasttech Wireless Network authorized users will be required to login and authenticate with their assigned Username and Password. Usernames and passwords will be assigned by STI's IT Department.

Please see the STI's Technology Resource Policy for additional details on acceptable usage relating to passwords.

Guests/Students with non-STI purchased laptop

STI Public Wireless Network

The STI Public Wireless Network is an open network which only Internet can be accessed. Campus resources such as printing and datacluster storage are not available. This network will be available to all guest machines on campus. Students who choose to bring their own laptop to campus will be considered guests and only have Internet access through their laptop. To gain access to other campus resources, students must log in with their STI username and password to a computer on campus which is on the STI secured network. All computer labs and public kiosks computers on campus will be available to all students and are connected to the STI secured network.

In order to access the STI Public Wireless Network users must accept and follow the STI Technology Acceptable Use Policy on the portal page before gaining access.

Security

All computers that are connected to the STI's Network in any way, whether owned by the user or STI, must be running approved anti-virus software with the latest virus updates. Extreme care must be taken when opening email attachments as they may contain a virus.

Approved anti-virus software by STI:

Norton AntiVirus
McAfee VirusScan Plus
Microsoft Forefront
Trend Micro Internet Security
AVG Anti-Virus



For security and network maintenance purposes, STI's IT Department may monitor and audit individual equipment, systems, and wireless network traffic at any time to ensure compliance with this policy.

STI's IT Department has the authority to disconnect any device from the wireless network that violates the practices set forth in this policy or any other related policy. It is the responsibility of the user to be knowledgeable of the information set forth in such policies.

Prohibited Use

All users are subject to the rules laid out in the STI's Technology Resource Policy and other relevant policies. Authorized personnel may be exempt from these restrictions during the course of their work (e.g.: Dept. of Information Technology staff may need to scan the network to troubleshoot performance issues). At no time is any STI student or employee to take part in any activity that is illegal under local, state, federal or international law while using STI's resources.

STI's IT Department is solely responsible for providing wireless networking services campus-wide. No unauthorized personnel or department may deploy wireless network access points or other wireless service on campus. Private wireless access points in Student Housing or offices are strictly prohibited.

Policy Enforcement

Violations of the rules set forth in this policy may result in the following disciplinary actions being taken by STI:

- Limiting of a person's access to some or all of the STI's resources.
- Initiation of disciplinary actions by STI up to and including, but not limited to, termination or suspension of employment or enrollment.
- Criminal prosecution under state and federal laws.

This policy will be reviewed on a regular basis and is subject to change as new technologies and methods of implementing these technologies emerge. Changes that are made to this document must be approved by the Southeast Technical Institute's Director of Information Technology/CIO and STI's governing bodies.

Revision History

February 1, 2008	Policy effective date
March 1, 2009	Added STI Public Wireless Network info